

**To Mitigate The Effect of EDoS Attack in Cloud
Computing**

A Dissertation Report Submitted

BY

Amita

(11307808)

to

**Department of Computer
Science**

In fulfilment of the Requirement for the
Award of the Degree of

**Master of Technology in Computer
Science & Engineering**

Under the guidance of

Mr. Kundan Munjal

(MAY, 2015)

PAC APPROVAL FORM



School of: Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMANCE

Name of the student : AMITA
Batch : 2013-2015
Session : 2014-2015

Registration No : 11307808
Roll No : RK2306850
Parent Section : K2306


Details of Supervisor:
Name : KUNDAN MUNJAL
UID : 16806

Designation : Assistant Professor
Qualification : M.Tech
Research Exp. : 2.5 year

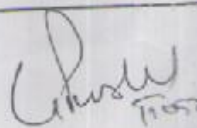
Specialization Area: DATABASE (pick from list of provided specialization areas by DAA)

Proposed Topics:-

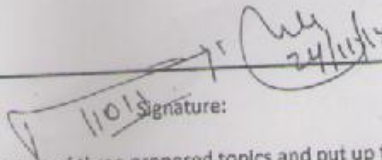
1. AN EFFICIENT SCHEME FOR PROVIDING SECURITY IN CLOUD COMPUTING
2. PROVIDING SECURITY AT DIFFERENT LAYERS IN CLOUD COMPUTING.
3. DATA HIDING IN CLOUD COMPUTING


Signature of supervisor

PAC Remarks: Topic 1 is approved


11057

APPROVAL OF PAC CHAIRMAN


Signature: 24/11/14

Date:

- *Supervision should finally encircle one topic out of three proposed topics and put up for an approval before Project Approval Committee (PAC).
- *Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/ Dissertation final report.
- *One copy to be submitted to supervisor.

ABSTRACT

Cloud computing is a new computing model that offers a number of services such as pay only for selected services hardware and software on rent .Cloud computing is a set of activity or IT services tin which we use computer hardware and software as well as others services that are provided over a network to a customer or client according to their requirements which are. Usually cloud computing services are offered by third parties provider who invest or buy own infrastructure. In addition to this, these services are typically in form of infrastructure as a service (Iaas), platform as a service (paas) and software as a service(saas). Its offers certain benefits such a as flexibility, scalability as well as innovative Business model for organizations to adopt IT services with minimal investment. owing to its increases in popularity , majority of new service providers are trying to implement this model , despite of these benefits, companies/ organizations/enterprises are not used to much extent due to certain reasons such as security issues and challenges associated with it. Security is one of major concern which prevent the growth of cloud .Apart from this, privacy, authentication, data security and confidentiality are also the pitfalls of cloud computing.

CERTIFICATE

This is to certify that **Amita** has completed M.Tech (Computer Science and Engineering) Dissertation titled “**To Mitigate the Effect of EDoS Attack in Cloud Computing**” under my guidance and supervision. To the best of my knowledge the present work is the result of his original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the fulfilment of the conditions award of M.Tech (Computer Science and Engineering) degree.

Date: _____

Signature of Advisor

Name: _____

UID: _____

ACKNOWLEDGEMENT

I am very grateful to my project guide **Mr.Kundan Munjal**, Asst. Prof. in Department of Computer Science & Technology, Lovely Professional University, for his extensive patience and guidance throughout my project work. Without his help i could not completed my work successfully. I would like to thank **Mr. Dalwinder Singh**, Professor and Head, Department of Computer Science and Engineering, Lovely Professional University, for having provided the freedom to use all the facilities available in the department, especially the library. I would also like to thank my classmates for always being there whenever I needed help or moral support. Finally, I express my immense gratitude with pleasure to the other individuals who have either directly or indirectly contributed to my need at right time for the development and success of this work.

DECLARATION

I hereby declare that the dissertation entitled, “**To Mitigate the Effect of EDoS Attack in Cloud Computing**” submitted for the M. Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: _____

Investigator

Regn. No. _____

TABLE OF CONTENTS

Sr. No	TOPIC	PAGE
1.	INTRODUCTION	1
	1. Introduction.....	1
	1.1 Deployment Model.....	7
	1.2 Services Model	9
	1.3 Characteristic	13
	1.4 Benefits.....	14
	1.5 Cloud Computing Challenges.....	15
	1.6 Security Issues In Cloud Computing.....	15
	1.7 Attack.....	17
2.	LITERATURE SURVEY	18
3.	PRESENT WORK	31
	3. Present work.....	31
	3.1 Scope of the study	31
	3.2 Problem formulation	31
	3.3 Objectives of the study	32
	3.4 Research Methodology.....	33
4.	RESULT AND DISCUSSION	35
	4. Result and discussion.....	35
5.	CONCLUSION AND FUTURE SCOPE	40
6.	REFERENCES	41
7.	APPENDIX	44
	7.1 List of abbreviations.....	44

LIST OF FIGURES

FIGURE.NO	TOPIC	PAGE
1.	Cloud Computing Deployment Model.....	9
2.	Cloud Computing Service Model.....	12
3.	EdoS Attack.....	17
4.	Without the Effect of EdoS attack.....	21
5.	Effect on Cloud Computing environment Existing approach	29
6.	Effect on Cloud of EdoS Attack by proposed approach.....	30
7.	Finish Time Under Attack.....	31
8.	Data overhaed0's complemented watermark image....	32
9.	Time Overhead	32
10.	Normal Finish Time	33

CHAPTER 1

INTRODUCTION

Cloud Computing is a collection of resources that are available for 24 hours as well as it can be accessible from anywhere through browser software all over the world. Cloud term is defined as a “virtual collection of computing resources”. We can define the cloud computing term means different things to different people. Distributed computing is a conveyed environment that provides high adaptable, versatile and constantly physical assets are given to customers as a service through web with greater flexibility and minimum infrastructure cost. Distributed computing gives everything in form of service.

Distributed computing in which a huge resources are dynamically allocated to the applications with aim of to offer these services to a maximum number of clients, we can expand or release our servers in size or accessibility but without spending costs in new infrastructure, training new personnel or licensing new software due to cloud computing, clients can lease these resources from a cloud provider as an outsourced service instead of investment on actual physical servers, storage and network equipment. Cloud computing is internet based computing, in which cloud service providers are charged to clients on the basis of usage of cloud service and network resources. Moreover, cloud allows the clients to maximize and minimize the number of requested resources as needed. Cloud Computing can also be defined as Application, Information as service and Management of Service over the cloud on demand. Cloud service providers require huge data centers around the globe for these applications and services which are delivered to customers by on the basis of demand through the internet and solid servers associated with what is cloud by facilitating web administrations and web applications. Cloud has a few highlights which include scalability, flexibility on demand and elasticity enable it to serve its clients. Due to these features, when clients adopt the cloud they can use some benefits directly. By Computing we are diminishing the expense, boosting storage limit, diminishing IT overhead and concerns, capacity to effortlessly impart data over the world. The customer can get to every one of these advantages by getting to the web.

As far as services are concerned, these are available on the basis of pay-per use where users pay only for those services which users want to use or access. Furthermore, in cloud models, users do not require to pay hardware and software maintenance cost. A number of companies related to cloud computing exist

such as Amazon, Google app engine, Microsoft window Azure, Sales force and others which they are in race to provide the optimum services to customers through this utility computing.

Distributed computing is a model for empowering helpful, on interest system access to an imparted pool of configurable processing resources (systems, servers, stockpiling, applications and services)that can be quickly provisioned and discharged with negligible administration exertion or administration supplier association.

Basic Concepts

There are certain service and model working to make cloud computing feasible and accessible for clients the following have been two models.

1.1 Deployment models

Deployment model tell us the type of access to cloud. Cloud computing operated four deployment models such as Public, Private, Community and Hybrid. Each deployment model have its own specific characteristics and features which suits to different cloud user. In cloud Deployment model, Networking, Platform, Storage and Software Infrastructure are provided as a service that is to minimize and maximize depending on demand.

1.1.1 Private Cloud: Private Cloud also known as internal clouds. This model is used solely for a private organizations/single organization, which is situated up inside an organization(internal information center).This cloud comprise on the facilitating of private applications and administrations for the private utilize just. In this model, It is easy to control over infrastructure, provide security and compliance that's are built and all managed by organizations itself. Cloud vendor provided scalable resources and virtual application, they are surveyed together and accessible for cloud client to impart and utilization. It contrasts from open cloud in that all cloud assets and applications are overseen by the associations itself, like intranet usefulness. This cloud offers the highest degree of control over performance, reliability and security. Private cloud can be more secure than others due to only organizations and specific users may have access for specific private cloud.

Cloud Computing Deployment Model

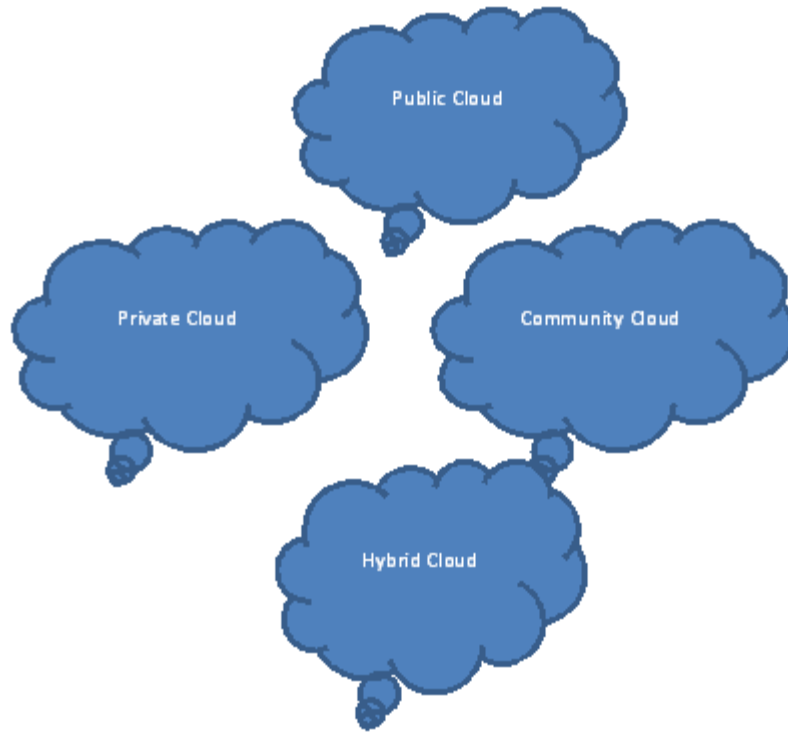


Fig 1.1

1.1.2 Public Cloud: Public cloud also known as external clouds A Public cloud is a model that provides services to general public over internet through certain interfaces by using mainstream web browser. Every utilization show that is like prepaid framework. By minimizing its capital expenditure on infrastructure, it helps the cloud users to better match their IT expenditure at an operational level. This cloud model is available for general public or a large enterprises group.

Public cloud offers several benefit to service providers includes:

- a) No Capital speculation on Infrastructure.
- b) Shifting of dangers to Infrastructure suppliers

As a result, this cloud lack controls over network and security settings, data which obstructs their effectiveness in many business scenarios. The main pitfall of this cloud is less secure than the other cloud models. It places an extra overhead of ensuring an application and data are accesses through public clouds are not matter of malicious attacks.

1.1.3 Hybrid Cloud: Hybrid cloud is a combination of both private and public cloud by which it provides virtual IT solutions .In this cloud part of the infrastructure service runs in a private cloud and remaining

part runs in public cloud. It is a private cloud linked to one or more external cloud services, centrally managed, in a single unit and circumstanced by secure network. It is more secure in case of data and applications as compared to public clouds. And it has an open architecture that allows various parties to access the information over the network. This deployment model provided various services such as networking, storage, platform and software infrastructure that can expand according to their utility. The main pitfall of this cloud designing of this cloud requires attention during the splitting between private and public cloud components.

1.1.4 Community Cloud: This deployment model supports a specific community that has shared objective (Such as security requirements, policy). It is accessible by several organizations or may be managed by internal organizations or a third party. It offers some services at low cost as that of private cloud. In this cloud, infrastructure shared between several organizations by means of this, they use share cloud resources and capabilities. The main pitfall of this cloud all the data is stored at one location, therefore it may be accessible by others.

1.2 Service Models:

Cloud computing is based on service models, we can observe that we require three users which are categorizes in this three ways:

1.2.1 End user/SaaS: SaaS is most popular choice for users SaaS is a software distribution model in which application are hosted by service provider and made accessible to end users via internet. Users can use certain application/software such as Ms Office, paint brush, Adobe photo shop that type of services provided to end users through a web browser via internet. SaaS is closely related to ASP(Application service provider) and on demand computing delivery models. users can access this services by pay per use according to their demand. In this case, users do not need to worry about cost and maintenance of these software instead these are all managed by cloud services providers. SaaS Providers are Salesforce.com, Rackspace.

Benefits Of SaaS Model:

- a) Simpler organization
- b) Automatic redesigns and patch administration
- c) Compatibility
- d) Easier Collaboration
- e) Global accessibility

1.2.2 Commercial organization/Iaas: Iaas is most basic level of service which it provides access to general resources such as physical machines, virtual machine and virtual storages. In this case, vendor shared dedicated resources with designated clients on basis of pay-per use fee. By this way, It reduces the investment in computer hardware such as a servers, storage device and processing power. For instance, suppose anyone wants to expand his business in own country as well as at international level through own website for this purpose who have to set up own servers for storage that’s lead to very high investment. It can be removed by Iaas In which maintenance ,housing and running of data services is provided by cloud services providers. The cloud owner who offers IaaS is called IaaS Provider which include Amazon EC2.

Components of Iaas Model:

- a) Broad network access
- b) Policy-based services
- c) Full scalability
- d) Desktop virtualization
- e) Automation of Administrative tasks

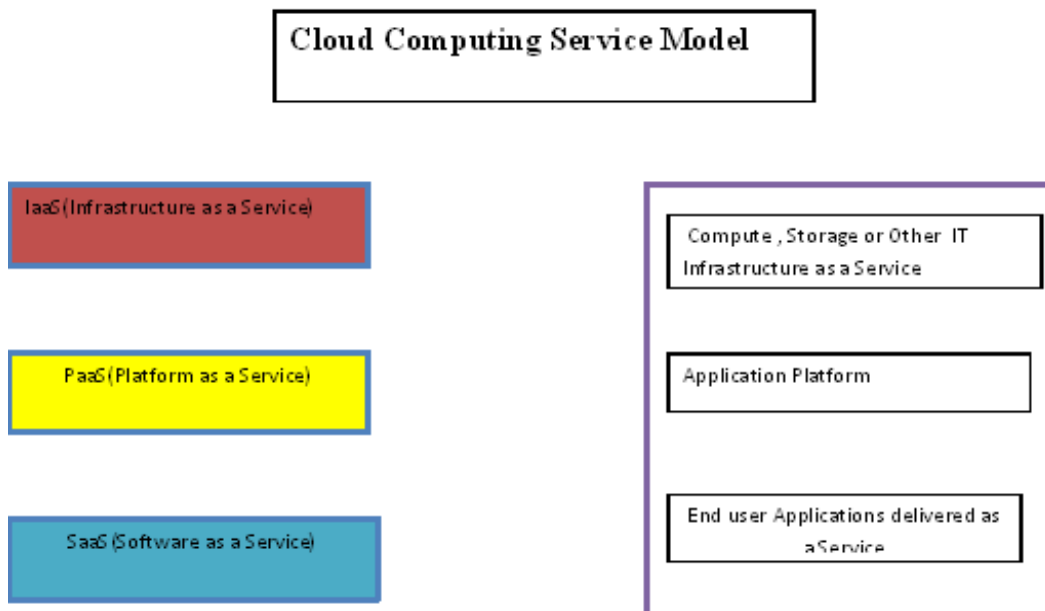


Fig 1.2

1.2.3 Developer/Paas:Paas work like as a Laas But it offers an additional function –“rented”. In Paas layer, virtual machines act as a catalyst in cloud computing. It must to protect the virtual machines against

malicious attacks such as a cloud malware. PaaS is a way to provide hardware ,operating systems, storage and network space on rent via internet. It allows the users use virtualized server and its associated services and testing new ones or developing on rent. It is must to understand the need of developer on which they wants to work with platform such as operating system. It services offered by paas. PaaS offers some benefits to developers such as frequently upgraded the features of operating system. Geographically distributed teams can work together on software development projects.Cloud provided tools /libraries to users by using these they creates the software. The users control the software deployment and configuration settings. PaaS refers to providing platform layer resources, including operating system support and software development frameworks. Example of PaaS providers include Google App Engine, Microsoft Windows Azure

Characteristics of PaaS Model:

- a) Multi-tenant Architecture
- b) Unlimited Database
- c) Programming user interface
- d) Flexible Integration model

1.3 Characteristics

1. **On demand service** Cloud computing enables the users to use its resources without any interaction between of other and also its provider. As a result, there is no need of human Interaction ,thus it improves efficiency and saving the cost for user as well as its provider.
2. **Broad network access** To provide a large pool of resources & services to a community of end users, it requires High bandwidth connection. For fulfill this , Many organizations or companies use 3 tier Architecture to establish a connection with cloud computing platforms such as Laptops, Printers.
3. **Location Independent resource pooling**The infrastructure providers are pooling to secure multiple users by using a multi- tenant Model, It dynamically assigned the resources to multiple consumers, According to their demand and reassigned. Such dynamically assigned resources provides flexibility to the providers in order to managing their own resources. These assets are situated in wide geographic areas physically & allot it essentially. Assets which can be incorporated as capacity ,handling memory, system, transfer speed & virtual machines.
4. **Measured Services** The amounts of monitories the cloud assets can be perform consequently. It can contact consequently and by utilizing a metering ability. Asset use can

be controlled & observed for supplier & purchaser by offering transparency .Furthermore , user have to pay only for those resources which are used by them and are constantly made mindful of any disparities , spikes or irregular conduct in regards to assets.

5. **Rapid Elasticity**Users can expand & compress their resources according to their requirements which can be done automatically. As a result, It shows that resources are infinite & application can cope when in demand. When customers do not require any resources they are relinquished back into resource pool.
6. **Service Oriented:**Distributed computing uses an administration driven working model and it put a solid effect on administration.. In a Cloud , Each provider offering its services as indicated by administration level assention arranged with its clients.. Therefore, SLA protection is not kidding or discriminating point of each administration supplier.
7. **Dynamic Resource Providing:**One of most important feature of cloud computing is that it can be obtained and released dynamic resource provisioning which offers services to their need or usage, It lead to lower the operating cost.
8. **Utility Based Pricing** Cloud computing emerged as a new innovative paradigm which offers services and resources over the internet. Thee exact pricing scheme may vary from source to source. Utility computing model offers cost to customers on the basis of usage. However, it also introduces complexities in controlling the operational cost.

1.4) Cloud computing Benefits

1. **Cost Savings :**

By using operational expenditures, companies can increase their computing capabilities and can decrease their capital expenditures. There are various reasons behind to uses Cloud innovation because of lower expenses. The charging model is pay as per the utilization of the model; the framework is not have to be acquired & bringing down upkeep. Beginning cost and repeating costs are much lower than traditional Computing.

2. **Scalability Flexibility**

Person can start companies with basic organization and expand to a substantial arrangement and return with same sending. In the event that it is vital, because of adaptable nature of distributed computing , it allows to utilize extra assets at crest times, empowering them to

pick up fulfill with client requests. This is an amazingly important characteristic for cloud computing, even all the more quickly, Cloud processing weights on getting applications to market quickly, by using the most suitable building pieces essential for sending.

3. Reliability

Different destinations can bolster business congruity & calamity recuperation with persistent accessibility by utilizing administrations.

4. Maintenance

Cloud service providers take the responsibility of software system maintenance & he/she do not require to install applications on the pc. By this approach, It further reduce the maintenance requirements.

5. Mobile Accessible

Due to system availability from any location, it have increased the productivity of mobile workers & Labors.

6. Increased Storage

Since the cloud can scale progressively, with the gigantic framework that is offered by providers.

1.5) Cloud Computing Challenges

1. Availability of Service:

Availability mean keep benefit ceaselessly with no intrusion or take the administration off. The appropriate fitting of this issue is giving the numerous cloud suppliers to business congruity or accessibility of the service in cloud. DDoS(Distributed Denial of Service) is another cause of availability of service. By using elasticity feature of cloud Computing, Cloud Computing can give the answer for safeguard against DDoS(Distributed Denial of Service).Cloud Computing moves the attack way from Saas supplier to the utility Computing supplier.

2. Security:

It is pass that the Security Issue has assumed the most critical part in thwart the acknowledgement of Cloud Computing. Many Security Issues Such as Data Loss, Phishing, botnet, It Pose serious threat to organizations. Multi-tenancy model and pooled Computing resources new Security Challenge that required new technique to tackle with these problems.

1.6 Security Issues In Cloud Computing

There are numerous favorable circumstances of Cloud Computing Such as time , Cost,innovation ,But Still there are Significant Security Issues of Cloud Computing. Major Security issues related to those faced by service providers and security Issues faced by their customers.

1. Location of data:
2. Access to data :
3. Security Breach: If a security incident occurs, What support will be provided?
4. Legal Issues
5. Authentication And Authorization

1.7Attack:

In the Cloud era, Companies are adopting cloud owing to they can use its best resources which are available in the market and its cost are reduced drastically. No doubt, Time, Cost, Innovation are the benefits of cloud computing, we have to address the security concerns when we use shared cloud environment. Major security issues faced by their customers and as well as by cloud providers(organizations providing platform or infrastructure as a service) through the cloud. Due to these security issues Many customers feel scare to opt it for their business concerns as well as for their other purposes.

Consequently security issue has played the vital role in acceptance of cloud computing .For instance, the network has interconnects the system in a cloud has to be secure. Without any doubt, share your data, running your software on someone else hard disk can appear to be harmful such as data loss, pose serious threats for an organizations. Cloud computing enable the attacker in grab of customers to rent out spaces on their physical machines at an hourly rent as well as more reliable infrastructure services at relatively cheaper for them to start an attack. Assurance of security in the cloud is a major challenge for the providers. The security can be administrated in the cloud at different levels and for several types of attacks. Cloud is prone to variety of attacks such DOS attack.

DOS is an major threat where users is granted partial or no access to his/her data. Companies can access cloud for 24*7 from anywhere, Dos can cause drastically increase in cost for users as well as for service

providers. Its is very uphill task to recognize the intended users from traffic attack. Detecting and filtering attack is a challenging task in an environment like cloud where everything is virtualized.

In the cloud, there are several types of attacks at network layer which provides harm to the network services and resources. DDOS is one of them, the main aim of this attack to create unavailability of network resources and prevent the intended users from accessing the network resources and services “ by consuming all available bandwidth”. Attackers have to use a large number of machine to launch distributed Dos Attacks by putting a overload on necessary network and CPU resources. As a cloud computing environment is highly scalable, the service will consume more resources during DDOS attack period to maintain service level of agreement. As a result, It contribute to revenue Loss .Thus the traditional DDOS attack can be transformed into EDOS attack in an Cloud environment .The EDOS

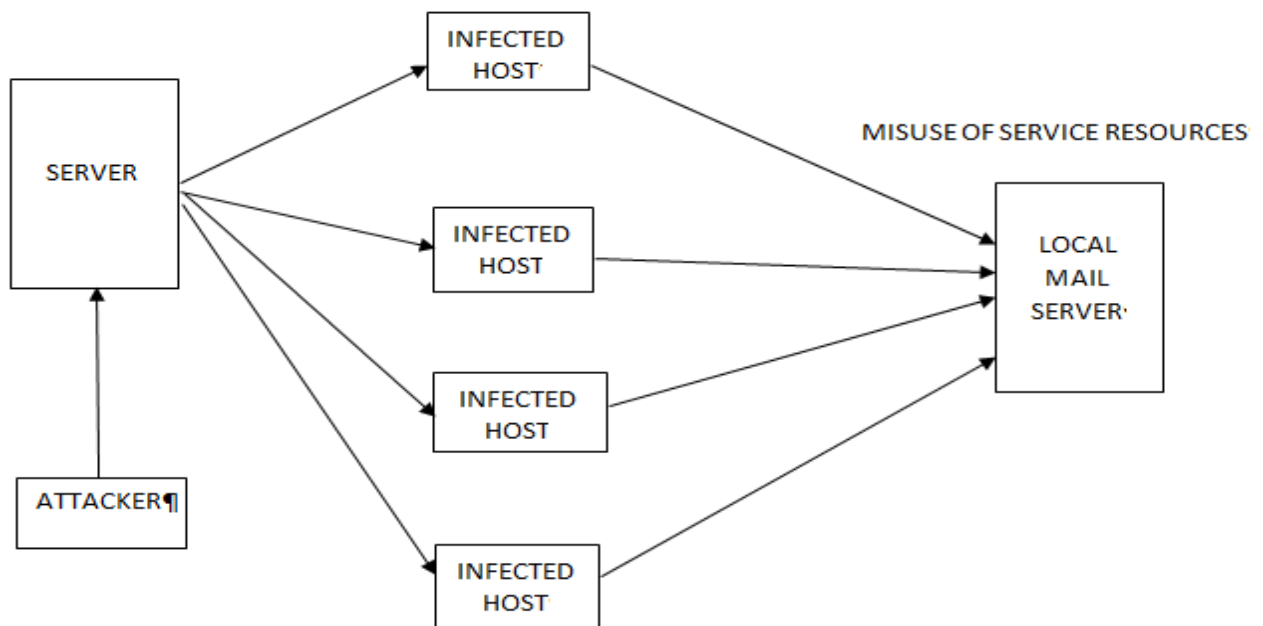


Fig 1.3

attack is a new breed of attack specifically targets the cloud environment

This Attack has been referred to EDOS while it is termed as Fraudulent Resource Consumption attack. This new type of attack targets the cloud adopter Economic resources. This attack appears as a version of low volumetric application layer DDOS attack. EDOS Attack does not objective to exhaust the victim bandwidth ,the main aim is to put a huge financial burden on victim through consumption of victim metered (pay as you go) bandwidth.

CHAPTER 2

Literature Review

RamgovindS[11], Presented a paper named “The Management of security in cloud computing”. This Paper specifically focused on cloud computing concerns as well on information security requirements. Cloud Computing has reached at new limits due to flexible and scalable features and offers data storage and capacity at lower costs. In addition to this, It highlights the cloud security issues that find by survey of international data corporation that based on cloud threats. The main aim of this paper is provide to overall security concerns. Owing to security issues Some customers feel scare to opt it for business scenarios. This Paper also describes the different types of cloud model, that is known as deployment model, Architectural delivery model, cloud computing concerns-cloud security issues, cloud shortfalls , information security requirements such as authentication and identification at each various cloud deployment and delivery model set out by vendors in highlight a very secure cloud framework. In this paper, Security Challenge which are currently faced in cloud computing industry are highlighted.

Munwar Ali zardari/Low Tang Jung/ M Nordin[13],(2013) Presents a paper as “ Data security study of market-oriented Cloud. According to this paper ,what types of issues weare still facing in deploying cloud models as well as in what way cloud security tools are meeting data security challenges and highlight the main CSP Such as Amazon and Soon. It explained a number of security issues such as data loss and data control in clouds. Data security and privacy issues arise with the number of users in cloud. Four major types of Clouds found which are widely used by users.

Qi Zhang Lu Cheng RaoufBoutaba,(2010),Presents a paper as ,”computing: State of the art and research challenges”. In this Paper they demonstrates its overview of cloud computing, Related Technologies, Business Model, Types of Clouds, and research challenges of cloud computing. In this paper , We have surveyed by highlight research challenges to draw attention from research community .As a result,It can bring Significant improvement or contribution in this field Provide immense benefits.

K.s.Suresh,2012[5],Presents this Paper ,named “ Security Issues and security Algorithms In Cloud Computing” Which provides a complete illustration of infrastructure, services, different security algorithms, security issues and attacks that are possible in cloud computing. Cloud computing is a technology in which uses computer hardware or software .Cloud computing is a set of IT service which are provided by third party who has owns infrastructure and offer to a customer over a network via internet. Usually, It is provided services in the form of Laas, Paas, Saas .This paper describes about overview of

different security Algorithms Such as MD5,RSA,AES By these algorithm providing user authentication . Moreover, This paper explain in brief about security Attack such as DDoS Attack.

Kuyoro S. O.[10], Presents this paper, named Cloud Computing Security Issues and Challenges. This paper a detailed of the cloud computing security issues and challenges as well as at the service delivery types. Cloud Computing offers a new innovative business model through which we use IT Services without any Investment on Infrastructure. This Paper highlight Security is one of major issues which act as obstacles in growth of cloud many security issue such as Data Loss,Phishing pose threat in Data and Software. Due to this, Organizations are in slow to accepting this phenomenon. In this era, many technologies are emerging at a pace in order to make a human life easier and comfort The customer needs to be aware about security risks and challenges that are related to this new environment. Cloud computing is no exception one.

Keiko Hashizum, Presents this paper named, ” An Analysis of Security Issues for Cloud Computing”. It presents the level of risk owing to essential services which are provided by outsider that makes it intense to keep up information security, Privacy, service availability and other services .It focus was to identify the main vulnerabilities ,countermeasures, risks and the most threats with possible solutions and traditional security solution do not act appropriate in case of malicious attacks so new approaches are necessary. Data security become a major concern when Saas users become totally reply on service Providers for security .In addition to this, Data is usually available in plain text in the cloud and also mention the Laas and Iaas security Issues in cloud.

KaziZunnurhain[12] , Presents this paper named ,”Security Attacks And Solutions in Cloud”.Cloud computing Posses many security issues ,attacks and risks. This paper highlight the security attacks related to cloud such as Wrapping assaults, Malware infusion assaults, Flooding assaults, Browser Attacks and distinguish the main drivers of these assaults in cloud and identify the solution of these attacks Such as Utilizing the Fat table. The concepts that discussed in this paper that helps in establish a new architecture for security in the cloud computing environment. This will surely attract more customers and vendors satisfaction to some extent.

ChiragModi,DhirenPatel,BhaveshBorisaniya(2012) ,Presents this paper named ,”A Survey on Security Issues And Solutions at different layers of Cloud computing. Cloud computing is a technology which offers a variety of services to end users via internet without spending much in infrastructure or licensing software. This paper highlight which factors affecting cloud computing adoption ,types of attacks which are exist in cloud and Identify the possible solution to improve the security in cloud environment. Discuss the survey on security issues at different layers of the cloud and what types of services affected due to these attacks and effects also their existing solution of these issues. This paper tells us many challenges

related to privacy and security are exist in this environment. It show various vulnerabilities ,threats and attacks that acts asa hinder while adopting the cloud Computing and survey about existing solutions to address the security issues. This paper helps the Providers and Clients to choose the right services from growing Cloud vendors.

S VivinSandar ,SudhirShenai[6],Presents this paper named, “Economic Denial of Sustainability (EDoS) in Cloud services Using HTTP and XML based DDOS Attacks”. This Paper throw some light on dangers and counter measures of ddos attacks in cloud environment and Cloud Specific vulnerabilities to these attacks. The administration was focused by DDoS assaults from a few hubs which prompt Consuming more Amazon administrations ,that prompt EDoS Attack(Economic Denial of Sustainability).This Paper illustrates the change of DDoS(Distributed denial of service) Attack into EDoS Cloud Specific Attack(Economic Denial of Sustainability).It explores the security Framework for EDOS Attack protection,which is clarified in two situations ,one with a genuine User and another with an assailant getting to the administration. The current methodology is not suitable to totally taking out the EDOS Attack. It is still required a enhance component to dispense with the Edos Attack from the Cloud.

WaelAlosaimi and Khalid Al-Begain[7], presents this paper named ,”A New Method to mitigate the Impacts of Economical Denial of Sustainability Attacks Against the Cloud “.In the field of cloud Computing, security has turned into a major challenge of concerns. T attacks such as distributed Denial of Service (Ddos) and the Economical Denial of Sustainability (Edos) are influence the pay-per use model, which is a standout amongst the most important advantageous of the cloud.with the presentation of new strategies in enterprise, for example, the "Bring Your Own Device" (BYOD)can again get to be extremely appropriate. Hackers can get access to the inner system by an endeavor to create Edos attacks against the cloud by misusing the nonappearance of a bound together administration of heterogeneous stages of the devices which are utilized as a part of the BYOD environment. Utilizing the cloud service provider (Indirect DDOS),it can influence the enterprise itself (Direct DDOS) or different enterprises. Consequently, To encounter Edos attacks, this paper use a schema called Ddos- Mitigation System (Ddos-MS) in which to verify the authenticity of the source, it check two packets that are coming from the source of requests (real or malignant). Graphic Turing Test (GTT) and Crypto Puzzles are two sort of tests are performed in this scenario .In this proposed schema, we are testing just two packets that are coming from any source rather than totesting all packets in order to reduce latency (end-to-end) Additionally, we perform two sorts of tests in which one verifies the client and rest one check the packet.

Mettildha Mary ,P.V Kavitha,Priyadharshini,Vigneshwer S Ramana[9] ,presents this paper named,” Secure Cloud Computing Environment Against DDOS and EDOS Attacks”.Cloud processing is turning into one of the quickest developing in the field of IT . Distributed computing permits us to scale our

servers in and accessibility to give administration to add noteworthy number of end clients. In addition, cloud administration model are charged focused around a pay-for every use premise of the cloud's server and system asset. In distributed computing in which infrastructure is imparted by possibly a large number of clients, Distributed Denial of Service (Ddos) attack can possibly have much more prominent effect than against single tenanted architectures. In Cloud Computing, a Ddos attack on server and system assets is changed into another type of attack that put impact on the cloud client's financial asset, to be specific Economic Denial of Service attacks. In this paper, highlight the Ddos and Edosshield, to keep away from the Denial of administration and Economic Denial of Sustainability (Edos) attack in the cloud computing .These attacks are easy to implement for attacker but for security experts require double efforts is difficult to stop.

MadarapuNaresh Kumar, P Sujatha ,VamshiKalva,RohitNagori[8] ,Presents this paper named ,” Mitigating Economic Denial of Sustainability (EDOS) in Cloud Computing Using In-Cloud Scrubber Service”.Cloud computing it is a better approach for conveying computing assets to end users. Flexible cloud computing enable administrations to be provided and accesses widely on the basis of demand of customers through internet with little maintenance. The Cloud-based Ddos assaults or outside Ddos assaults can make apparently genuine solicitations for a support of produce a monetary Distributed Denial of Service (eddos) –where due to the flexible way of the cloud that permits scaling of servicebeyondthemethod for the attendant to pay their cloud-based service bills which prompts Economic Denial of Sustainability (Edos). This issue can be tended to by eddosmitigation service (scrubber Service) for relieving DDOS attacks at the application-layer and system layer DDOS attacks through proficient cloud puzzle approach.

FirasD.Ahmed,Amer AI Nejam,Presents this paper named ,”Cloud Computing :Technical Challenges And CloudSim Functionalities”. Big organizations are performing the rapid development in era of internet in order to lessen their expense of correspondence, stockpiling and figuring.

Cloud computing is one of them, which offer different services Such as reliable ,secure, fault-tolerant, sustainable and Scalable with also offers Software, infrastructure and platform as services .Instead of storing the data and software application files on local /personal computer , it put away on remote servers through the association with the web. This Paper discuss all the concepts of cloud computing such as definition ,sorts,, benefits, characteristics and measure the specialized and non specialized difficulties of distributed computing.

MohitKumar,Nirmal Roberts, Presents this paper named ,” A Technique to reduce the Economic Denial of Sustainability (EDOS) Attack in Cloud Computing”. The most broadly utilized innovation of today's reality is Cloud Computing. Distributed computing is a gathering of assets (mix of

programming and equipment) which is given to the customers on the pay each usage preface by web. Essentially it provides three sorts of services, such as software as a service (SaaS), platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud gives the office to expand and compress its servers; stockpiling and so forth and can give administration to huge number of appeals. Cloud gives these benefits to its users in computing environment. But it enhances the chance of vulnerability. Therefore providing security in Cloud computing is one of the significant issue for service provider and defenseless issue in distributed computing is distributed Denial of Service (DDoS) attack and consuming of cloud resource attack is changed into a new attack, it is known as a Economic Denial of Sustainability (EDoS). Its objective is to use the cloud resource and put the financial burden on others /the authentic client. EDoS attack is not the same as DDoS attack. The primary objective of EDoS attack is to break down the victimized person's financial plan, not to crash the server.

Fahd Al-Haidari Mohammed H. Sqalli, presents this paper named, "Improved EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses". Cloud computing is the one of the quickest developing IT sections. A cloud presents platforms, where clients have to Pay only for those resources which are used by users known as "pay-as-youuse". With this model, a customary DDoS attack focusing on servers and system resources is changed in a cloud situation to another attack that targets the cloud adopter's financial asset, specifically Economic Denial of Sustainability (EDoS) attack. In this paper, we propose an arrangement as an upgrade of Existing work, in particular EDoS-Shield, to relieve the EDoS attacks beginning from spoofed IP addresses. We outline a discrete experiment to check its execution and the outcomes demonstrate that it is an answer for alleviate the EDoS attacks beginning from spoofed IP addresses. The improved EDoS-Shield procedure beats the first EDoS-Shield as far as execution and expense measurements.

Zubair A. Baig, Farid Binbeshr, Presents this paper named, "Controlled Virtual Resource Access to Mitigate Economic Denial of Sustainability (EDoS) Attacks Against Cloud Infrastructures." Administration suppliers of the cloud have seen a quickly developing interest to give administration to clients in an opportune way. Security vulnerabilities of the cloud system can't be neglected. Through abuse of such shortcomings, the foe class may disturb cloud operations, and have a weakening impact on the notoriety of the administration supplier. One attack sort particularly influencing cloud administrations is the Economic Denial of Sustainability (EDoS) attack. By such a malignant attack, the ability of the service supplier to alertly extend and accommodate expanding numbers of requests coming by end-clients, is abused, to make it monetarily unviable for the service supplier to maintain further interest for administration from real end-clients. In this paper, we propose a novel methodology for specifically controlling client demands for service, actualized at

the administration supplier's end. In this plan, we lessen i.e alleviate the impacts of an up and coming EDoS attack against discriminating cloud assets. Approaching appeals are arranged into typical or suspicious. Therefore, further examination is directed to guarantee that need to cloud administration access is given to those end-clients labeled as being genuine, while, suspect clients are given lesser need to administration access, until they are in the end expelled from the suspect list. simulations ,we are led to study the execution of the plan, with results indicating guarantee.

Mo hammed H. Sqalli Fahd Al-Haidari presents this paper named, "EDoS- Shield –A two Steps Mitigation Technique against Edos Attacks in Cloud Computing ".Cloud computing is currently most of the one built up data innovation fields. Cloud computing permits to expand or compress the servers in extent and accessibility to give administration to a more noteworthy of users. In addition, users have to pay only for those services which are used by them, otherwise known as utility Computing. With this model, a conventional DDoS attack on server and which is changed in a cloud computing to another type of attack that put a economic burden on innocent user Economic Denial of Sustainability attack(EDoS). In this paper, we Propose a arrangement, named EDoS-Shield, to relieve the Economic Denial of Sustainability (EDoS) attack in the cloud computing frameworks. **Joseph Idziorek, Mark Tannian, Doug Jacobson** presents this paper named, " Attribution of Fraudulent Resource Consumption in the Cloud" .Dissimilar to an application-layer DDoS attack that expends assets with the objective of upsetting short-term accessibility, a FRC attack is a extensively more inconspicuous attack that rather tries to disturb the long haul money related suitability of working in the cloud by abusing the utility valuing . By falsely expending cloud resources in Large volume (i.e. information exchanged), an attacker (e.g. botnet) has the capacity bring about huge deceitful charges for the exploited(victim) person. This paper discuss a procedure to distinguish noxious customers partaking in a FRC attack. Trial results show that the introduced procedure accomplishes qualified accomplishment against challenging attack situations.

Anusha K, Tulasiram N, Mary SairaBhanuS, Presents this paper named, "Detection of Economic Denial of Sustainability using Time Spent on a Web Page in Cloud".Cloud computing is a manifestation of utility computing where the purchasers leverage figuring assets. Charging is done on an hourly premise taking into account the measure of assets expended. On account of web servers the expense is based on the amount of information that leaves the web server and the quantity of HTTP asks for received. The cloud administration supplier naturally scales the assets when there is a climb in shoppers movement and the expense on the purchaser increments as needs be. to application supplier. Consequently, creating a manageable decrease in the economy of the customer, in fact named as Economic denial of Sustainability(EDoS). The http movement created by the generated by the attacker mimics the genuine traffic so as to go undetected.

This paper proposes a discovery instrument in view of the Time Spent on a Web Page(TSP) characterized as time spent on review a website page. The TSP of the assault movement varies from the mean TSP of a website page. This deviation of TSP from the mean is ascertained taking the exponential dispersion of the TSPs and the calculated value is utilized to recognize the surreptitious conduct.

Muddassar Masood, Zahid Anwar, Syed Ali Raza, Muhammad Ali Hur, Presents this paper named, "EDoSArmor: A Cost Effective Economic Denial of Sustainability Attack Mitigation Framework for E-Commerce Applications in cloud Environments ". The guarantee of usage model of cloud computing has attracted in an extensive number of medium what's more, little undertakings to receive E-Commerce model of directing on-line organizations. E-Commerce applications on the Cloud grow organizations by making them all the more generally open, they likewise makes these applications vulnerable to economic denial of sustainability attacks - a form of application layer DDoS attack that drive up the expense of Cloud computing by spending application assets.

This paper concentrates on recognition and relief of EDoS for E-Commerce based applications. EDoS is not the same as conventional DDoS in that, the plan of the recent is to consume all the resources (like memory, data transfer capacity, CPU and so on) of the Web Server in this way making it occupied to its honest to actual clients. EDoS then again is brought on by malicious clients who are not intrigued by taking after the normal work process of an E-trade application by buying things yet by utilizing it for their own purposes of amusement, value checks and idle surfing. We have a twofold arrangement, (i) confirmation control and (ii) congestion control. In the initially, we farthest point number of customers that can at the same time send demands, hence permitting just enough customers that can be served effortlessly inside accessible assets on the Web server. In the second, we change the need of permitted customers in light of the sort of assets they visit and sort of exercises they perform, in this manner making the most extreme assets accessible to great customers. We have incorporated and assessed this arrangement in a Web Application Firewall and discovered it very viable in term of assets circulation among customers going from great and terrible customers.

Nisha H. Bhandari Presents this paper named, "Survey on DDoS Attacks and its Detection & Defence Approaches" In Cloud environment, cloud servers giving requested cloud benefits, generally may crash in the wake of getting tremendous measure of heap of appeals. This situation is called Denial Of administration assault . Distributed computing is one of today's most invigorating developments on account of its capacity to overcome costs joined with figuring while growing versatility and adaptability for PC forms. Cloud processing is changing the IT movement model to

give on-interest self-Service access to a bestowed pool of handling resources (physical and virtual) by method for wide framework access to offer reduced costs, limit use, higher efficiencies and portability. Starting late Distributed Denial of Service (DDoS) assaults on Cloud has transformed into one of the authentic dangers to this murmuring advancement. Conveyed Denial of Service (DDoS) assaults continue torment on the Internet. Disseminated Denial-of-Service (DDoS) assaults are a basic issue in light of the way that they are hard to perceive, there is no thorough course of action and it can cut off a relationship from the Internet. The vital goal of an assault is to deny the misused individual's passageway to a particular resource. In this paper, we have to overview the current DoS and DDoS ID and resistance instrument.

KaziZunnurhain and Susan V. Vrbsky presents this paper named, "Security Attacks And Solution in Cloud". Distributed computing offers additional standard potential to enhance benefit and reduce costs, however meanwhile it has various new security threats. In this paper we recognize the possible security attacks on Cloud including: Wrapping assaults, Malware-Injection assaults, Flooding assaults, Browser assaults, besides Accountability checking issues. We perceive the basic main drivers of these attacks and propose specific plans.

Distributed Computing is upsetting how information development resources and administrations are used and administered. We have depicted some key and doubtlessly comprehended security assaults and have proposed some potential plans in this paper, for instance, utilizing the FAT table and a Hypervisor.

Gehana Booth, Andrew Soknacki, and Anil Somayaji presents this paper named, "Cloud Security: Attacks And Current Defenses". This paper shows an unusual state request of current research in Cloud computing security. Unlike past work, this portrayal is created around attack frameworks and contrasting boundaries. Specifically, we outline a couple danger models for Cloud processing systems, discuss specific attack frameworks, and arrange proposed guards by how they address these models and counter these instruments. This examination highlights that, while there has been broad exploration to date, there are still genuine risks to dispersed processing systems, for instance, potential establishment exchange off, that need to be better had a tendency to.

Zhifeng Xiao and Yang Xiao, presents this paper named, "Security and Privacy in Cloud Computing". Late Improvements have offered ascent to the fame and accomplishment of distributed computing. Be that as it may, when outsourcing the information and business application to an outsider ascents the security and protection issues. All through the current learn, the creators acquire a typical objective to give complete audit of the current security and protection issues in cloud situations. We have distinguished five most illustrative security and protection characteristics (i.e., classifiedness, uprightness, accessibility, responsibility, and protection preservability).

Starting with these properties, we display the connections among them, the vulnerabilities that may be abused by assailants, the risk models, and also existing safeguard methods in a cloud situation. Future examination headings are beforehand decided for every quality.

Manas M N, Nagalakshmi C K, ShobhaG presents this paper named, "Cloud Computing Security Issues And Methods to Overcome". Distributed computing is an innovation which fulfills clients dynamic asset requests and makes the employment simpler to chip away at all stages for the client. Distributed computing is the conveyance of figuring administrations over the Internet. Security is the principle criteria when taking a shot at cloud, as the outsider inclusion will be there. Secure structural planning ought to be utilized to give benefits through the cloud. The broad utilization of virtualization in executing cloud foundation brings remarkable security attentiveness toward clients or occupants of an open cloud administration. Virtualization changes the relationship between the OS and basic equipment - be it processing, stockpiling or notwithstanding systems administration. Strategies demonstrate to defeat the security issues of the cloud".

AbhishekGoel, ShikhaGoel presents this paper named, "Security Issues in Cloud Computing "The new generation of devices and technologies has brought drastically change in everything . The work on the go culture is getting involved in day to day activities. The cloud computing plays an important role in bringing the no need to purchase the hardware. The Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a web through the internet. The key security issue with in the clouds is that the owner of the data may not have control or not aware about of where and how the data is placed. As if anyone wants to take uses of the cloud, he must ensure the secure network and also utilize the resource allocation and scheduling provided by clouds. The secure data exchange is crucial for any network; so it is very important to take security and privacy into account when designing and using cloud services. In this paper security in cloud computing is elaborated in a way that covers security issues, concerns and challenges for Data Security in Cloud. In this paper, Threats to cloud confidentiality, cloud integrity, cloud availability& cloud privacy and related issues are discussed.

B.Vani,R.Cynthia Monica Priya, presents this paper named, "A Survey on the Security Issues in Cloud Computing". Cloud computing is a one of fast growing paradigm that deals with hosting and delivering services as well as resources over the internet. In order to reduce both the software and hardware burden, Virtualization provides the end users a variety of services from the hardware to the application level. The pay peruse model is the most distinguished feature of the cloud Computing. The another remarkable feature of Cloud Computing to scale the computing infrastructure up and

down Location transparency, resource pooling, ubiquitous network access are these important characteristics of cloud computing. Everything has certain pros and cons It is also one of them which suffers from certain weakness. This paper highlight the various security issues such as confidentiality, integrity and availability.

Palvinder Singh, Er. AnuragJain presents this paper named, "Security Issues and Challenges in Cloud Computing". Cloud computing is an emerging computing Paradigm that gives the concept of users services with attractive technological and with the lower costs. The infrastructure uses new technology and services that haven't been absolutely evaluated with security. In this paper, discuss the impacts of the distinctive characteristics of cloud computing such as multi-tenancy, elasticity and third party management, upon the protection necessities. Then, analyze the need of security in cloud Computing in terms of confidentiality, integrity, convenience, trust, and audit and compliance.

Anand Darne1, RushikeshLongadge presents this paper named, "A Result Analysis on Secured Encryption in Cloud Computing using Symmetric Cryptography". The paper talks about all the consequences of protection and security of distributed computing. We have executed every one of these parameters as essential cloud application and its organization. Fundamentally We have executed property driven security model for distributed computing. Our application has the capacity beat the assaults from different fields over privacy, respectability, accessibility, responsibility, and security preservability. Distributed computing gives countless advantages to its clients however it neglects to comprehend security Parameters particularly in broad daylight cloud. Symmetric Cryptographic Key is delicate information and it is obliged to be put away at cloud stage to take care of a few issues of scrambled information, for example, seeking/control on encoded information. This paper is introducing a procedure that will oversee symmetric cryptographic keys on cloud-based environment. We have distinguished five most illustrative security and protection traits (i.e., classifiedness, uprightness, accessibility, responsibility, and protection preservability). Starting with these characteristics, we exhibit the connections among them, the vulnerabilities that may be misused by aggressors, the risk models, and also existing protection techniques in a cloud situation. Future examination bearings are beforehand decided for every characteristic.

VinkoZlomislic presents this paper named "Denial of Service Attacks" Denial of service (DoS) attacks present one of the most significant threats to for secure information systems. Requires resourcefulness in designing and implementing reliable defenses owing to the Rapid development of new and increasingly sophisticated attacks This paper discusses an overview of current DoS attack and defense concepts, from a theoretical and practical point of view. Main directions are proposed for

future research required in defending against the evolving threat and also considering the elaborated DoS mechanisms

- i. **Zubair A. Baig, Farid Binbeshr** presents this paper named, “controlled virtual resource access to mitigate EDoS attacks against cloud infrastructure”. In Cloud Computing , a rapidly growing demand to provide services to end-users in a timely manner have been noticed by Service providers of the cloud. Security vulnerabilities against the cloud infrastructure cannot be ignored. Through exploitation of such weaknesses, it can disrupt routine cloud assets, and have a negative impact on the reputation of the service provider. One attack type specifically affecting cloud services is the Economic Denial of Sustainability (EDoS) attack. Through such a malicious attack, the ability of the service provider to dynamically stretch and accommodate increasing numbers of requests from end-users, and put the financial burden on victim. In this paper, we propose a approach for selectively controlling user requests for service, implemented at the service provider's end. By this scheme, we reduce i.e. mitigate the effects of an imminent EDoS attack against cloud resources. Incoming requests are divided into normal or suspicious. Consequently, further analysis is conducted to ensure that p cloud service access is given to those end-users whose has been identified as being legitimate, while, suspect users are given lesser priority to service access, until they are eventually removed from the suspect list. Subsequently, ithelps to secure the legitimate end users from the such attacks etc.& delays found is to be minimal.

The work has completed to mitigate the effect of EDoS Attack in Cloud Environment. This process as implemented in the Cloudsim& Java.

3.1 Scope of the Study

Cloud Computing is an emerging technology in which unlimited resource and data can be stored as per Requirements due to its elastic nature. But on the other hand, This field is still facing some problem of secure communication inside the cloud. The programmers may aim by launching the DDos attack to damage the system resources and cause unavailability for others and in some case it impose a huge burden on service provider which may cause the economic issues of the specific firm. These attacks are called EDoS attacks or economical denial of sustainability, which particularly influence the popularity of the application specific. By implementing a such scenarios, system is able to identify/detect the requests user that is legal or fraud and also by removing of EDoS attack from cloud environment, security of utility cloud model will be enhanced. Moreover, as a result of it also remove the communication hurdle between the cloud nodes or cloud server-user communication. By following these schema, Cloud Computing can maintain/ revive and/or retain the performance of the services offered by the cloud service providers and also to remove the economic losses which are faced by cloud provider in case of fraudulent resource consumption. By mitigate the effect of EdoS attack, enhanced the security of cloud Computing and also controlled access guarantees can be provided to all cloud users. Moreover, by reducing the EDoSAttack, to control access to the end users, for mitigating the effects of an Edos Attack.

3.2 Problem formulation

Cloud Computing has been popular topic for researches in the last 10 years. Cloud Computing is an emerging technology in which unlimited resource and data can be stored as per Requirements due to its elastic nature. But on the other Hand, This field is still facing some problem of secure communication inside the cloud. The Ddos attacks are performed for the most of part by the gathering of programmers with a specific end goal to accomplish some specific

objective. The programmers may aim the Ddos attack to damage the system dependency and asset accessibility of some specific online service provider, which may cause the economic issues of the specific firm. These attacks are called Edos attacks or economical denial of sustainability, which particularly influence the popularity of the application specific. These attacks can result in major security issues, accidents, movement blockage, and so on. These attacks cause the unavailability of the resources or can cause the malicious injection in the cloud applications.

DoS (Denial of Service) Attacks are caused by flooding of many packets as a result of which is communication hurdle between the cloud nodes or cloud server-user communication. In order to maintain/ revive and/or retain the performance of the services offered by the cloud service providers and also to minimize the economic losses, these attacks have to be checked regularly in the highest possible effective manner. Furthermore, there is no doubt, there are various framework which are proposed for Edos attack that is Cloud specific attack. But Existing protection framework are not able to detect and completely remove this attack from the cloud. This field require still more research in order to enhance a better and secure framework to secure the cloud from these sorts of attacks.

3.3 Objective of the Study

1. To get the robust Client Puzzle scheme which works in this environment and gives the minimal delays.
2. To focus on a Client Puzzle scheme that provides fair control for Cloud resources. It provides security for the cloud resources.
3. The existing system uses certain methods for the reduce/mitigate the effects of an EdoS attack Which provide the security against the many others attacks and this is one of the robust approach.
4. To improve the more security to the Cloud Computing the proposed algorithm. Proposed Algorithm are applied on the Cloud Environments so that it will mitigate the effect of Malicious attacks during the demand of service by end-users.
5. Proposed algorithm will helps to secure the legitimate end users from the such attacks etc.

3.4 Research Methodology

The methodology in this proposal is to achieve the research is the hybrid approach. This approach presents the mixture of descriptive and exploratory methodologies. These two approaches are useful

to achieve the good results in the research. The Exploratory approach is used for collecting the information about the techniques which are using in the image digital watermarking. From the above approach the collecting data will help to achieve good image watermarking techniques. Descriptive analysis is used to achieve the problems in the existing system it provides some methodology which help in solving the problems which are defined by the researcher. Descriptive and Exploratory approaches are used to solve the any type of problems which were produced by the researchers in the real world.

1. Qualitative Approach

In the qualitative approach we study related to the Security Issues and attacks in Cloud computing. Providing security is become major challenge to cloud clients from different sorts of attacks. Cloud computing is a technology that are provided to end clients via internet and in which customer pay to service providers for those services that are used by them. In addition to this, these services are an attractive target for attackers , they use all available resources and bandwidth and cause unavailability of services for other customers by DDOS attack. Moreover, hackers bringing about new stress for the service providers by imposing the economic losses for fraudulent resource consumption ,it is termed as EDOS Attack that is cloud specific attack.

2. Quantitative Approach

In the quantitative analysis we are going to design and define the algorithm we are using to detect and remove the new breed of DDoS Attack Which is known as EDOS attack(FRC) From the recent study and approach which is used till now in the literature survey is the several Proposed Framework in which explain the use of virtual Firewall that is start point for the cloud and Client puzzle server that is a used in mitigate the Distributed denial of service. and also illustrate the two scenarios for EDos Attack in which one for actual client and remaining one for fraud. They are not able to provide better results. The existing framework are not capable to provide accurate results. we still need of research in order to can provide better and secure framework to cloud from such attacks.

Mixed Approach

This is basic approach that which includes both approach which includes the qualitative approach and quantitative approach. The basic terminology that combining the both approaches is detect the Edos attack and prevent from the fraudulent resource consumption (FRC).

Proposed Algorithm

1. Node X1 sends the request to the neighbor request to node X.
2. Node X examines the location of node X1, and permits them to join the Cloud server application.

3. Node X examines the packet stream, its size and payload information.
4. If packet size remains same for every packet, it examines the payload information. If payload information is found same in two packet of a single communication stream, it is marked as possible attacker.
5. If the number of same packets increase a certain limit, the sender node is marked as the EDoS attacker and the information is provided to all of the nodes in the cluster.
6. All nodes are updated to block the attacker node and stop receiving the packets from the attacker node.

CHAPTER 4

RESULTS AND DISCUSSIONS

Cloud computing is not a secure utility model owing to its security issues. By using Edos shield techniques, we try to verify the requests user whether source of requests is legal or fraud. The main aim to stop the consumption of victim metered bandwidth by attacker that is termed as fraudulent resource consumption(FRC) that is cloud specific attack. To obstruct the misuse of the utility pricing model of cloud that doing by launching an attack as a type of DDoS attack. It have to become Like that pricing model of utilities in which client have to pay only for those amount of services which is used by them such as Electricity. The adversary aim to use the victim bandwidth for long term which is offered by cloud service provider to client that is pay to him on basis of usage. By using these technique, System will able to detect the fraud who uses the offered services by cloud provider in the grab of genuine Client and also obstruct the fraudulent resource consumption. and also Client service providers will not affected by Edos Attack as well as will not lose their own customers.

```
520.1: GlobalBroker_: Cloudlet 104 received
520.1: GlobalBroker_: Cloudlet 109 received
520.1: GlobalBroker_: All Cloudlets executed. Finishing...
520.1: GlobalBroker_: Destroying UM #100
520.1: GlobalBroker_: Destroying UM #101
520.1: GlobalBroker_: Destroying UM #102
520.1: GlobalBroker_: Destroying UM #103
520.1: GlobalBroker_: Destroying UM #104
GlobalBroker_ is shutting down...
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for shutting down.
Datacenter_0 is shutting down...
Datacenter_1 is shutting down...
Broker_0 is shutting down...
GlobalBroker_ is shutting down...
Simulation completed.
Simulation completed.

===== OUTPUT =====
Cloudlet ID   STATUS   Data center ID   UM ID   Time   Start Time   Finish Time
0            SUCCESS   3                0       320    0.1          320.1
5            SUCCESS   3                0       320    0.1          320.1
1            SUCCESS   3                1       320    0.1          320.1
6            SUCCESS   3                1       320    0.1          320.1
2            SUCCESS   3                2       320    0.1          320.1
7            SUCCESS   3                2       320    0.1          320.1
4            SUCCESS   3                4       320    0.1          320.1
9            SUCCESS   3                4       320    0.1          320.1
3            SUCCESS   3                3       320    0.1          320.1
8            SUCCESS   3                3       320    0.1          320.1
101         SUCCESS   3                101    320    200.1        520.1
106         SUCCESS   3                101    320    200.1        520.1
103         SUCCESS   3                103    320    200.1        520.1
108         SUCCESS   3                103    320    200.1        520.1
100         SUCCESS   3                100    320    200.1        520.1
105         SUCCESS   3                100    320    200.1        520.1
102         SUCCESS   3                102    320    200.1        520.1
107         SUCCESS   3                102    320    200.1        520.1
104         SUCCESS   3                104    320    200.1        520.1
109         SUCCESS   3                104    320    200.1        520.1
CloudSimExample8 finished!
C:\c\cloudsim>
```

```

320.1: Broker_0: Cloudlet 5 received
320.1: Broker_0: Cloudlet 1 received
320.1: Broker_0: Cloudlet 6 received
320.1: Broker_0: Cloudlet 2 received
320.1: Broker_0: Cloudlet 7 received
320.1: Broker_0: Cloudlet 4 received
320.1: Broker_0: Cloudlet 9 received
320.1: Broker_0: Cloudlet 3 received
320.1: Broker_0: Cloudlet 8 received
320.1: Broker_0: All Cloudlets executed. Finishing...
320.1: Broker_0: Destroying UM #0
320.1: Broker_0: Destroying UM #1
320.1: Broker_0: Destroying UM #2
320.1: Broker_0: Destroying UM #3
320.1: Broker_0: Destroying UM #4
Broker_0 is shutting down...
520.1: GlobalBroker_: Cloudlet 101 received
520.1: GlobalBroker_: Cloudlet 106 received
520.1: GlobalBroker_: Cloudlet 103 received
520.1: GlobalBroker_: Cloudlet 108 received
520.1: GlobalBroker_: Cloudlet 100 received
520.1: GlobalBroker_: Cloudlet 105 received
520.1: GlobalBroker_: Cloudlet 102 received
520.1: GlobalBroker_: Cloudlet 107 received
520.1: GlobalBroker_: Cloudlet 104 received
520.1: GlobalBroker_: Cloudlet 109 received
520.1: GlobalBroker_: All Cloudlets executed. Finishing...
520.1: GlobalBroker_: Destroying UM #100
520.1: GlobalBroker_: Destroying UM #101
520.1: GlobalBroker_: Destroying UM #102
520.1: GlobalBroker_: Destroying UM #103
520.1: GlobalBroker_: Destroying UM #104
GlobalBroker_ is shutting down...
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for shutting down.
Datacenter_0 is shutting down...
Datacenter_1 is shutting down...
Broker_0 is shutting down...
GlobalBroker_ is shutting down...
Simulation completed.
Simulation completed.

===== OUTPUT =====
Cloudlet ID  STATUS  Data center ID  UM ID  Time  Start Time  Finish Time  Time Overhead  Data Overhead
0            SUCCESS  3              0      320   0.1         360.1        40             100000
5            SUCCESS  3              0      320   0.1         360.1        40             100000
1            SUCCESS  3              1      320   0.1         360.1        40             100000
6            SUCCESS  3              1      320   0.1         360.1        40             100000
2            SUCCESS  3              2      320   0.1         360.1        40             100000
7            SUCCESS  3              2      320   0.1         360.1        40             100000
4            SUCCESS  3              4      320   0.1         360.1        40             100000
9            SUCCESS  3              4      320   0.1         360.1        40             100000
3            SUCCESS  3              3      320   0.1         360.1        40             100000
8            SUCCESS  3              3      320   0.1         360.1        40             100000
101         SUCCESS  3              101     320   200.1       560.1        40             100000
106         SUCCESS  3              101     320   200.1       560.1        40             100000
103         SUCCESS  3              103     320   200.1       560.1        40             100000
100         SUCCESS  3              100     320   200.1       560.1        40             100000
105         SUCCESS  3              100     320   200.1       560.1        40             100000
102         SUCCESS  3              102     320   200.1       560.1        40             100000
107         SUCCESS  3              102     320   200.1       560.1        40             100000
104         SUCCESS  3              104     320   200.1       560.1        40             100000
109         SUCCESS  3              104     320   200.1       560.1        40             100000
CloudSimExample8 finished!
C:\>cloudsim>

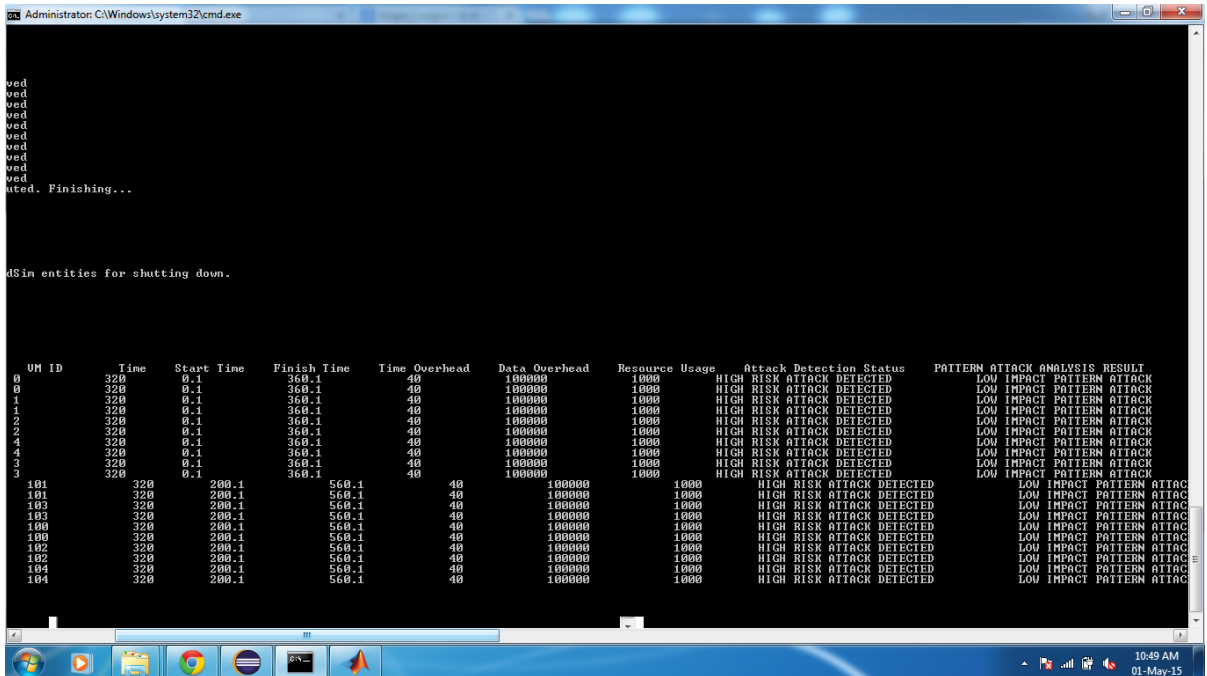
```

```

Administrator: C:\Windows\system32\cmd.exe
320.1: Broker_0: Destroying UM #3
320.1: Broker_0: Destroying UM #4
Broker_0 is shutting down...
520.1: GlobalBroker_: Cloudlet 101 received
520.1: GlobalBroker_: Cloudlet 106 received
520.1: GlobalBroker_: Cloudlet 103 received
520.1: GlobalBroker_: Cloudlet 108 received
520.1: GlobalBroker_: Cloudlet 100 received
520.1: GlobalBroker_: Cloudlet 105 received
520.1: GlobalBroker_: Cloudlet 102 received
520.1: GlobalBroker_: Cloudlet 107 received
520.1: GlobalBroker_: Cloudlet 104 received
520.1: GlobalBroker_: Cloudlet 109 received
520.1: GlobalBroker_: All Cloudlets executed. Finishing...
520.1: GlobalBroker_: Destroying UM #100
520.1: GlobalBroker_: Destroying UM #101
520.1: GlobalBroker_: Destroying UM #102
520.1: GlobalBroker_: Destroying UM #103
520.1: GlobalBroker_: Destroying UM #104
GlobalBroker_ is shutting down...
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for shutting down.
Datacenter_0 is shutting down...
Datacenter_1 is shutting down...
Broker_0 is shutting down...
GlobalBroker_ is shutting down...
Simulation completed.
Simulation completed.

===== OUTPUT =====
Cloudlet ID  STATUS  Data center ID  UM ID  Time  Start Time  Finish Time  Time Overhead  Data Overhead  Resource Usage  Attack Detection Status
0            SUCCESS  3              0      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
5            SUCCESS  3              0      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
1            SUCCESS  3              1      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
6            SUCCESS  3              1      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
2            SUCCESS  3              2      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
7            SUCCESS  3              2      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
4            SUCCESS  3              4      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
9            SUCCESS  3              4      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
3            SUCCESS  3              3      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
8            SUCCESS  3              3      320   0.1         360.1        40             100000          1000             HIGH RISK ATTACK DETECTED
101         SUCCESS  3              101     320   200.1       560.1        40             100000          1000             HIGH RISK ATTACK DETE
106         SUCCESS  3              101     320   200.1       560.1        40             100000          1000             HIGH RISK ATTACK DETE
103         SUCCESS  3              103     320   200.1       560.1        40             100000          1000             HIGH RISK ATTACK DETE
100         SUCCESS  3              100     320   200.1       560.1        40             100000          1000             HIGH RISK ATTACK DETE
105         SUCCESS  3              100     320   200.1       560.1        40             100000          1000             HIGH RISK ATTACK DETE
102         SUCCESS  3              102     320   200.1       560.1        40             100000          1000             HIGH RISK ATTACK DETE
107         SUCCESS  3              102     320   200.1       560.1        40             100000          1000             HIGH RISK ATTACK DETE
104         SUCCESS  3              104     320   200.1       560.1        40             100000          1000             HIGH RISK ATTACK DETE
109         SUCCESS  3              104     320   200.1       560.1        40             100000          1000             HIGH RISK ATTACK DETE
CloudSimExample8 finished!
C:\>cloudsim>
C:\>cloudsim>
C:\>cloudsim>

```



Effect of EDoS attack in cloud computing

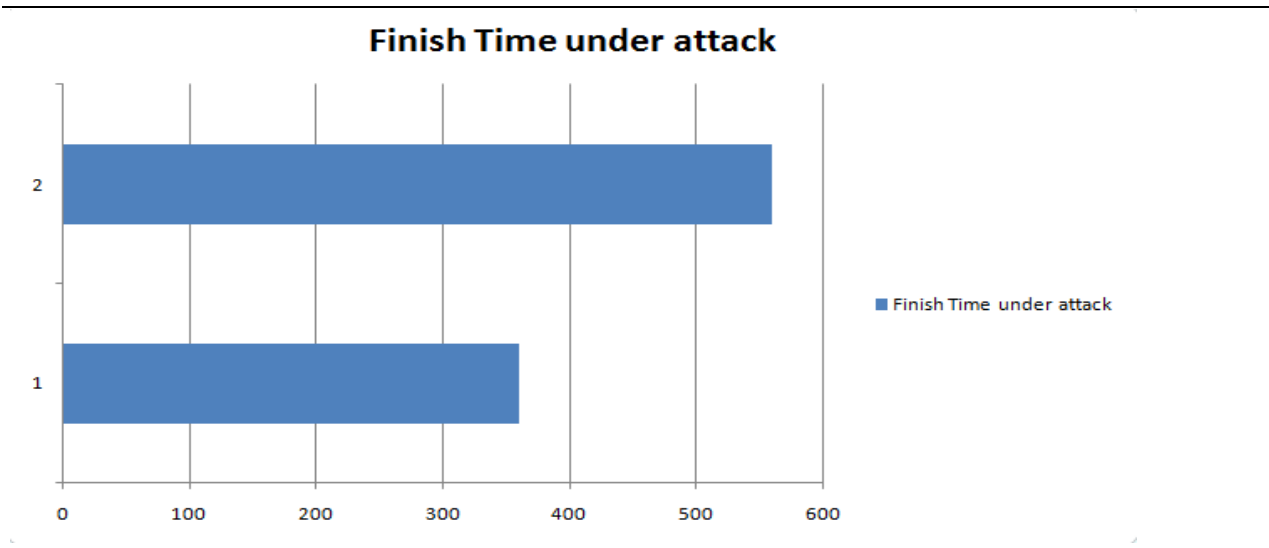


Fig: 4.1

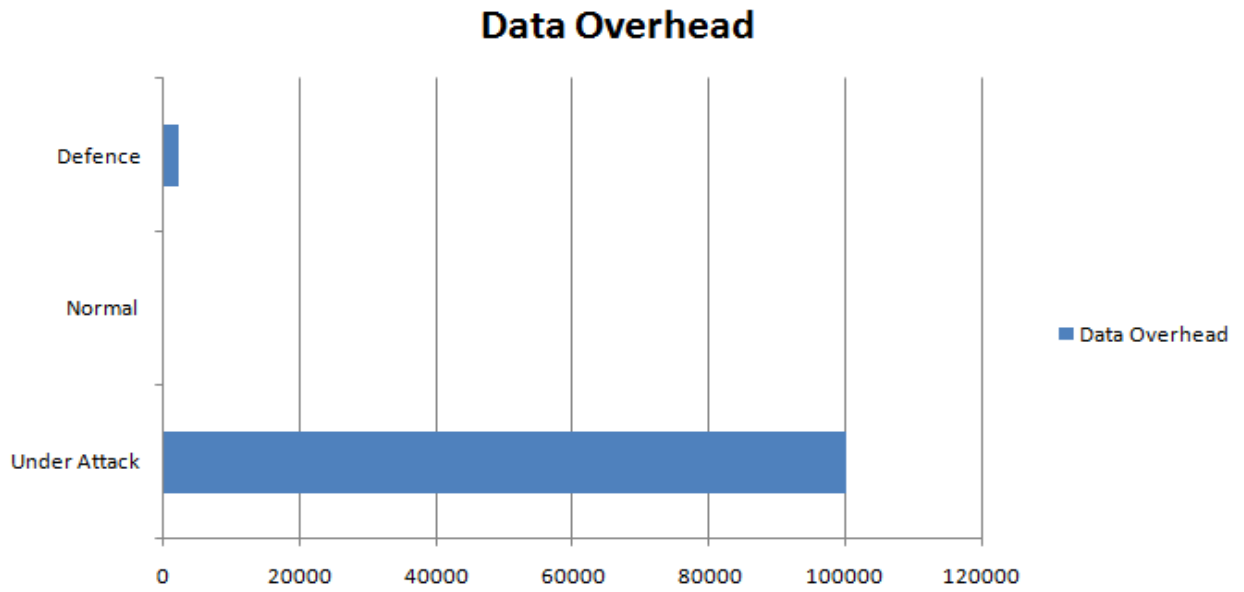


Fig:4.2

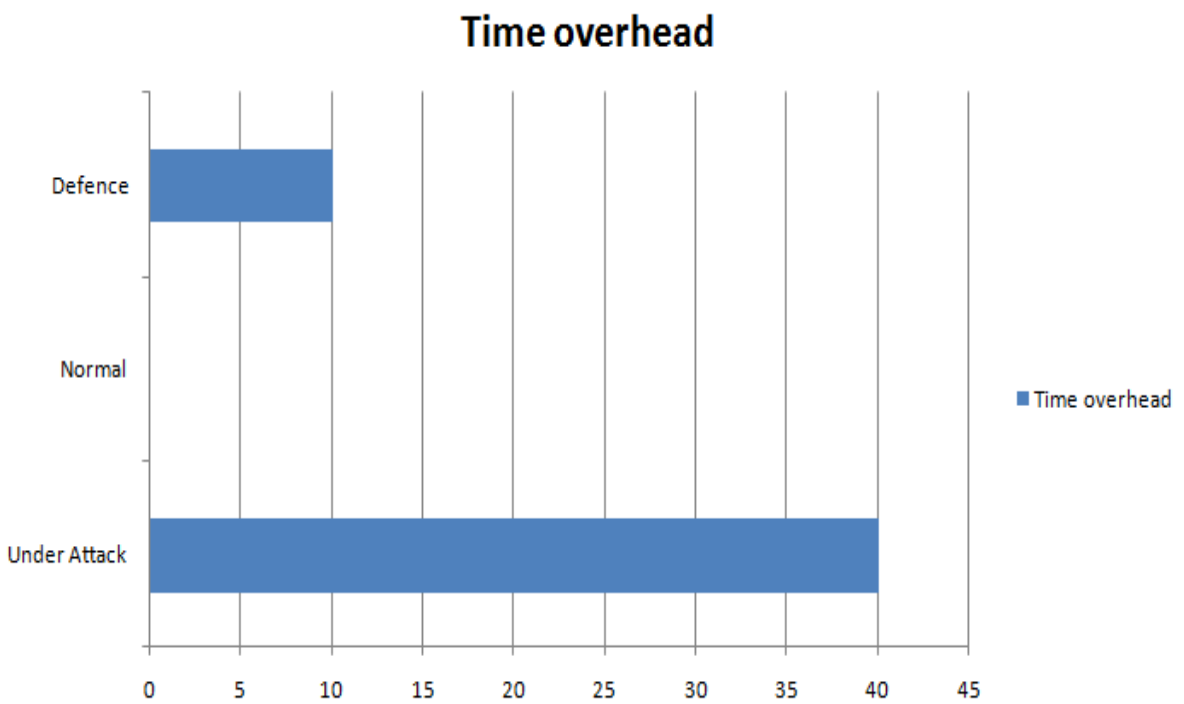


Fig: 4.3

Without EdoS Attack

Normal Finish Time

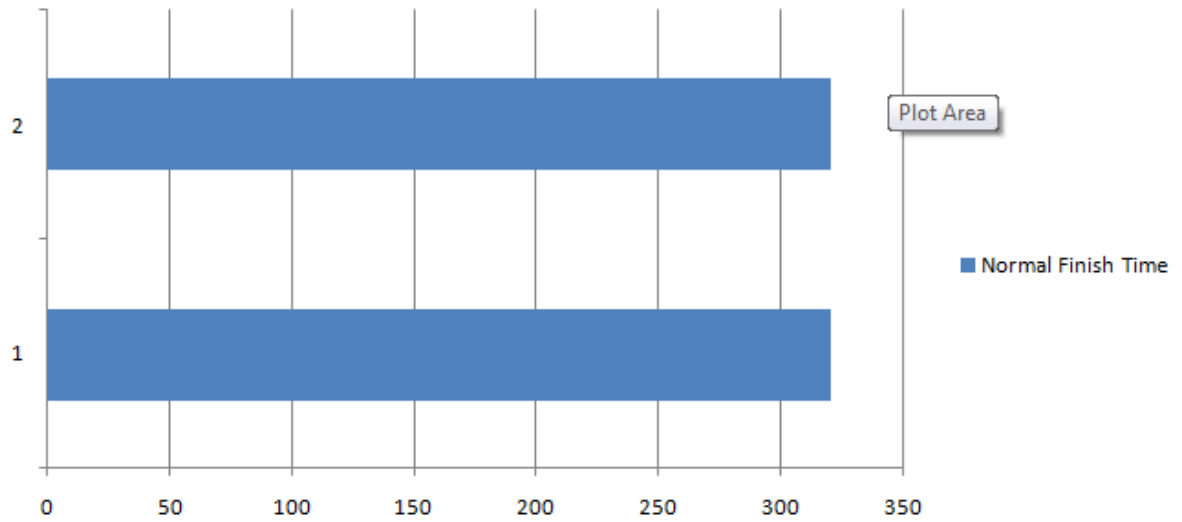


Fig : 4.4

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

Conclusion

The distributed computing model can scale computer resources on interest, and give clients various preferences to advancement their routine cluster framework. As a result, the aggregate expense of going towards cloud is practically resources are not being used. It tries to be enhanced as compared to the current solutions, and dodges their limits to deliver a strong and viable way against Edos attacks. New Approaches are required which ought to be a disseminated and versatile (scalable) methodology. New type of attacks are available in the cloud. A standout amongst the most danger threats in distributed computing security itself originates from Distributed Denial of Service attacks it is Edos attack really which is a new type of Ddos attack. The Edos attack exists just in the Cloud so it is named as one of the Cloud particular attack. These sorts of attack are basic and simple created by the hacker, however to security specialists they are require twice efforts to stop it.. The denial of-service attack have ended up more focused on services of cloud computing, bringing about new stresses for the service providers of cloud- by constraining them to pay service for serving fraudulent customers so as to keep up the SLA of a customer. The Existing methodologies are not equipped for totally taking out the Edos Attack. There are different types of the best methodologies to shield the ddos&Edos attacks. Keeping in mind the end goal to overcome such attacks we have to proposed an in-cloud Edos mitigation service which will be utilized on-interest a released as per pay-for every utilization premise.. There by decreasing the cloud-based bills to the service supplier and ensured accessibility of services can be guaranteed. The existing Approache is not capable of completely eliminating the EDoS attack.

CHAPTER 6

REFERENCES

- [1] Bernd Grobauer, Tobias Walloschek and Elmarstocker “understanding Cloud Computing vulnerabilities” Cloud Computing, Copublished by the IEEE Computer and Reliability Societies.
- [2] Mohammed H.Sqalli Fahd AlHaidariKhaledSalah ,”EDOS-Shield – A Two-Steps Mitigation Technique against EDOS Attacks in Cloud Computing “,Fourth IEEE International Conference on Utility and Cloud Computing.
- [3] Ashley Chonka , Yang Xiang n, Wanlei Zhou, AlessioBonti,” Cloud Security defence to protect Cloud Computing Against HTTP-DoS and XML-DoS Attacks”, Journal of network and computer Applications 34(2011)1097-1107
- [4] Meiko Jensen ,J”orgSchwenk,NilsGruschka,Luigi Lo Lacono,”On technical Security Issues in Cloud Computing “, IEEE International Conference on Cloud Computing.
- [5] K.S.Suresh ,K.V.Prasad,2012”Security Issues and Security Algorithms in Cloud Computing”, International Journal Of Computer Science and Software Engineering 2(10),pp 110-114
- [6] Vivinsandar ,S And Shenai S,2012 “Economical Denial of Sustainability(EDOS) in Cloud Services using HTTP and XML based DDOS attacks, International Journal of Computing Applications41(20),pp 11-16
- [7] WaelAlosaimi and Khaht Al-Begain ,”A New Method to Mitigate the Impacts of Economical Denial of Sustainability Attacks Against the Cloud”, ISBN (2013) PGnet
- [8] MadarapuNaresh Kumar, P.Sijatha, VamshiKalva, RohitNagori ,Anil Kumar KatuKojwala(2012),” Mitigating Economic Denial of Sustainability (EDoS) in Cloud Computing using In-Cloud scrubber Service “,Fourth IEEE International Conference on Computing Intelligence and Communication Networks
- [9] Mettildha Mary , P.V Kavitha, Priyadharshini M, Vigneshwar S Ramana,”Secure Cloud Computing Environment against DDoS and EdosAttacks”,International Journal of Computing Science and Information Technologies 5(2),pp 1803-1807
- [10] KuyoroS.Oibikunle F , AwodeleO.,”Cloud Computing Security Issues and Challenges”, International Journal of Computing Network 3(5),pp 247-255

- [11] damgovindS, Eloff MM, Smith E, "The Management of Security in Cloud Computing", (2010) IEEE
- [12] KaziZunnurhain and Susan V.vrbsy, "Security Attacks and Solutions in Cloud".
- [13] MunAliZardari, Low Tang Jung, M.Nordin B Zakaraia, "Data Security Analysis of market oriented Clouds", IEEE conference on wireless sensors
- [14] M.A.Morsy, J.Grundy and Muller I, "An analysis of the Cloud Computing Security Problem", In procApsec 2010 Cloud
- [15] FirasD.Ahmed, Amer AI Nejam, "Cloud Computing Technical Challenges and CloudsimFunctionalities", ISSN 2319-7064
- [16] MohitKumar, Nirmal Roberts, "A Technique to Reduce the Economic Denial of Sustainability (EDoS) attack
- [17] Sqalli, MohammedH.Fahd AI-haidari and khaledSalah, "EnhancedEDoS-Shield for MitigatingEDoS Attacks originating from IP Spoofed Address. In ,2012 IEEE 11th International Conference on Trust ,Security and Privacy in Computing and Communication IEEE, PP,1167-1174.
- [18] C. Hoff. Cloud computing security: From ddos (distributed denial of service) to edos (economic denial of substainability). [http://rational security.typepad.com/blog/2008/11/cloud-computing-security-from-ddos-distributed-denial-of-substaina.html](http://rationalsecurity.typepad.com/blog/2008/11/cloud-computing-security-from-ddos-distributed-denial-of-substaina.html),2008.
- [19] Kahate, Atul cryptography and network Security. TataMc-Graw-Hill Education, 2003.
- [20] William Stallings, "Crptography and network Security Priniciples and practices", Prenticehall, New Delhi.
- [21] Soon HinKhor and Aki Nakao, spow: On-demand Cloud-based eddos mitigation mechanism. In In proc.of the fifth workshop on hot topics in system dependability, 2009.
- [22] K.dutta, R.BGuin, S.Chakrabarti, S.Banerjee, and U.Biswas. A smart job scheduling system for cloud computing environments.
- [23] K.Prakash, "A Survey on security and privacy in Cloud Computing," Vol 2 Issue, February 2013.
- [24] M.Zhou, R.Zhang, W.Xie, WeiningQ. and A,Zhou, "Security and privacy in Cloud Computing: A Survey", Sixth International Conference on Semantics, knowledge and Grids, 2010
- [25] Haltonw(2010) SecurityIssues and Solutions in cloud Computing. [Http://wolfhalton.info/2010/06/25/security issues and solutions in cloud computing/](http://wolfhalton.info/2010/06/25/security-issues-and-solutions-in-cloud-computing/)
- [26] NaruchitparamesJ, Gunes MH(2011) Emhancing data Privacy and integrity in the cloud. in: HPCS, pp427-434

- [27] ZunnurhainK,vrbsky S(2010) Security attacks and solutions in clouds.IN:Proceedings of the 1st international conference on cloud computing,pp145-156.
- [28] Balachandra Reddy Kandukuri,RamkrishnaPaturiV,DR.AtanuRakshit,"Cloud Security Issues",2009 IEEE International Conference on Services Computing.
- [29] HuimingYu,NakiaPowell,DexterStembridge and Xiao HongYaun,"Cloud Computing and Security Challenges",2012 ACM Publication
- [30] Kamal Dahbur,Bassil Mohammad and Ahmad BisherTatakji,"in Cloud Computing 'A survey of Risks, Threats and Vulnerabilities in cloud computing.'"
- [31] FarzadSabahi Cloud Computing Security Threats and Responses
- [32] Farah Bashir Shaikh and SajjadHaider,'Security Threats in cloudComputing",In 6thInternational Conference on Internet Technology and Secured Transactions,2011.

List of abbreviations

IaaS-“Infrastructure as a Service”

PaaS-“Platform as a Service”

SaaS-“Software as a Service”

SOA –“Service Oriented Architecture”

EDOS-“ Economic Denial of Sustainability”

DDOS –“Distributed Denial Of Service”

CSP –“Client Service Provider”